AMENDMENTS TO THE SPECIFICATION:

On page 1 of the specification, replace the title beginning on the line numbered 1 and ending on the line numbered 3 with the following new title:

TRANSMISSION OF ENCRYPTED MESSAGES BEWTEEN A TRANSMITTER AND A RECEIVER UTILIZING A ONE-TIME CRYPTOGRAPHIC PAD

On page 2 of the specification, replace the paragraph beginning on the line numbered 28 and ending on page 3 on the line numbered 6 with the following paragraph:

When a message is to be sent, the sender uses the secret key to encrypt each character, one at a time. If a computer is used, each bit in the character (which is usually eight bits in length) is exclusively "OR'ed" with the corresponding bit in the secret key. (With a one-time pad, the encryption algorithm ~~maybe~~ may be implemented simply by using the XOR operation.) Where there is some concern about how truly random the key is, it is sometimes combined with another algorithm such as ~~MD5.)~~ MD5. This kind of encryption can be thought of as a "100% noise source" used to mask the message. Only the sender and receiver have the means to remove the noise. Once the one-time pad is used, it can't be reused. If it is reused, someone who intercepts multiple messages can begin to compare them for similar coding for words that may possibly occur in both messages.

On page 5 of the specification, replace the paragraph beginning on the line numbered 16 and ending on the line numbered 18 with the following paragraph:

The invention is seen to have a number of objects and ~~advantages, the~~ advantages. The first object and advantage is that the invention implements a one-time pad between communicating ~~pairs; the~~ pairs. The advantages and security benefits of a one-time pad are well-known.

On page 7 of the specification, replace the paragraph beginning on the line numbered 3 and ending on the line numbered 13 with the following paragraph:

During the process of preparing to transmit and receive messages, the communicating pair engage in a private protocol to establish a connection, choose parameters required to modulate-demodulate signals, and to synchronize communications. During this process, the communicating pair exchange information regarding internal data, as stored in internal data structures, and states that are private and common to the communicating pair and are independent of the content of transmitted messages. Either private internal data or some portion of a previously exchanged message is used by the communicating pair to negotiate a one-time pad. This information, whether a message, part thereof, or private internal data is hereafter ~~is~~ called a transmission, to distinguish from messages that are sent in response to a using device of the communicating pair.

On page 7 of the specification, replace the paragraph beginning on the line numbered 14 and ending on the line numbered 21 with the following paragraph:

With reference to Figure 2, the first transmitter-receiver executes the first of a series of steps 2000 to set up the pad. The first transmitter-receiver 2100 randomly selects a reference to one of the plurality of encryption devices. For example, the reference may <u>be</u> a number that designates the cryptographic device, or a pointer to a cryptographic software object having methods called to encrypt and decrypt data. The first transmitter-receiver retrieves a previous transmission received from the second transmitter-receiver 2200, then 2300 encrypts the previously received transmission using <u>the</u> randomly selected encryption device.

On page 7 of the specification, replace the paragraph beginning on the line numbered 29 and ending on page 8 on the line numbered 5 with the following paragraph:

The first transmitter-receiver 2400 randomly selects a reference to some previous transmission sent by the first transmitter-receiver to the second transmitter-receiver, <u>and</u> then 2500 encrypts the reference and constructs a message 2600, which is sent to the second transmitter-receiver. The previous transmission in this case is selected from the group consisting of: (a) a previous referenced message sent ~~by~~ <u>to</u> the second transmitter-receiver; (b) a predetermined portion of a previous referenced message sent ~~by~~ <u>to</u> the second transmitter-receiver; and (c) prespecified internal data that is generated by the communicating pair, that is independent of message content.

On page 8 of the specification, replace the paragraph beginning on the line numbered 9 and ending on the line numbered 20 with the following paragraph:

With reference to Figure 3000, the second transmitter-receiver 3100 receives the encrypted transmission, and discovers 3200 the cryptographic device used by the ~~first.~~ first transmitter-receiver. Discovery can be made in several ways, with one example being the second transmitter-receiver sequentially uses all its cryptographic devices, in turn, to decrypt the transmission received from the first transmitter-receiver. The second transmitter-receiver will have identified the cryptographic device used by the first transmitter-receiver when it is able to recover the transmission previously sent by the first transmitter-receiver that is known to second transmitter-receiver. Since the number of cryptographic devices is small in number, for example, less than twenty, the number of computational steps is relatively small to discover the cryptographic device used by the first transmitter-receiver, by sequential trial and error, although other methods are conceivable.

On page 9 of the specification, replace the paragraph beginning on the line numbered 10 and ending on the line numbered 16 with the following paragraph:

With reference to Figure 4, 4100 the first transmitter-receiver receives the encrypted transmission from the second transmitter-receiver, then using the encryption device selected by first transmitter-receiver, the transmission previously sent by the second transmitter-receiver is decrypted 4200 and 4300 is confirmed or disconfirmed by the first transmitter-receiver. The state of the confirmation is reported 4400, and if confirmed, the one-time pad, or cryptographic device is used to encrypt and transmit the current message.

On page 9 of the specification, please delete the title "DISCLOSURE SUMMARY" beginning and ending on the line numbered 18.